



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,586	06/19/2006	Benjamin Morin	33901-200PUS	1443
27799 7590 01/22/2009 COHEN, PONTANI, LIEBERMAN & PAVANE LLP 551 FIFTH AVENUE SUITE 1210 NEW YORK, NY 10176				
EXAMINER				
DOAN, TRANG T				
ART UNIT		PAPER NUMBER		
2431				
MAIL DATE		DELIVERY MODE		
01/22/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/583,586

Applicant(s)

MORIN ET AL.

Examiner

TRANG DOAN

Art Unit

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10/10/2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 June 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/ISD)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____
- Paper No(s)/Mail Date _____

DETAILED ACTION

1. This action is in response to the amendment filed on 10/10/2008.
2. Claims 1-6, 8-9 and 11-13 have been amended.
3. Claims 1-13 are pending for consideration.

Response to Arguments

4. Applicant's arguments with respect to the 35 U.S.C. 101 rejection have been fully considered but are not persuasive, therefore Examiner has maintained the 35 U.S.C. 101 rejection.
5. Applicant's arguments with respect to the 35 U.S.C. 112 2nd paragraph rejection have been fully considered in view of the amendment filed on 10/10/2008, which has been made in record, and Examiner has withdrawn the 35 U.S.C. 112 2nd paragraph rejection.
6. Applicant's arguments with respect to the Claim Objections have been fully considered in view of the amendment filed on 10/10/2008, which has been made in record, and Examiner has withdrawn the Claim Objections.
7. Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed

invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

8. In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

9. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new ground(s) of rejection.

Specification

10. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicant fails to provide proper antecedent basis for the terminology "a computer-readable medium" recited in claim 11.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

13. Independent claim 11 currently recites "a computer-readable medium encoded in a computer program...", first, it is not clear that the computer-readable medium is a software or hardware component. Since nowhere in Applicant's specification defines the computer-readable medium as the hardware component, Examiner broadly interprets the computer-readable medium as a software per se. Software is descriptive material per se and is not statutory because computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. (see MPEP 2106.01).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Julisch ("Clustering Intrusion Detection Alarms to Support Root Cause Analysis") (hereinafter Julisch) in view of Connary et al. (US 2004/0044912) (hereinafter Connary).

16. Regarding claim 1, Julisch discloses a method of managing alerts (Julisch: pages 467-468) issued by intrusion detection sensors of an information security system including an alert management system, each alert being defined by an alert identifier and an alert content, which method includes the following steps: associating with each of the alerts issued by the intrusion detection sensors a description including a conjunction of valued attributes belonging to attribute domains (Julisch: page 449, paragraph 2, "where $\{A_1, \dots, A_n\}$ is the set of alarm attributes ... alarm attributes capture intrinsic alarm properties, such as the source IP address or an alarm, its destination IP address, its alarm type (which encodes the observed attack), and its time-stamp"); organizing the valued attributes belonging to each attribute domain into a taxonomic structure defining generalization relationships between said valued attributes, a plurality of attribute domains forming a plurality of taxonomic structures (Julisch: page 449, paragraphs 2-4, "dom(A_i) is the domain (i.e., the range of possible value) of attribute A_i " and "generalization hierarchies"); completing the description of each of said alerts with sets of values induced by the taxonomic structures based on the valued attributes of said alerts to form complete alerts (Julisch: page 449, paragraphs 2-4, "generalized alarm"); and storing said complete alerts in a logic file system to enable said complete alerts to be consulted (Julisch: page 450, section 4 [ALARM-CLUSTERING PROBLEMS] and pages 456-457, section 5.1 and 463-465, "alarm log").

Julisch does not explicitly disclose wherein each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic. However, Connary discloses wherein each complete alert is

saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic (Connary: paragraphs 0092 and 0097).

Therefore, It would have been obvious to a person skilled art at the time the invention was made to have included in Julisch the feature of Connary as discussed above because it would be desirable to provide a network security system, apparatuses, methods, and articles with the capability to adjust threat levels associated with certain attacks customized to the nature of the network and its devices in a particular implementation. Moreover, it would be desirable to permit the network administrator to set the threat level and/or logic resulting in generation of alerts associated with network events to provide automated detection of security incidents (Connary: paragraph 0006).

17. Regarding claim 2, Julisch as modified further discloses wherein the complete alerts are consulted by at least one of successively interrogating and browsing said complete alerts so that the alert management system responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request to enable said request to be refined (Julisch: pages 464-465 and 467-468, section 7).

18. Regarding claim 3, Julisch as modified further discloses wherein the pertinent valued attributes assigned a highest priority are those that are most general, given the taxonomic structures (Julisch: page 464).

19. Regarding claim 4, Julisch as modified further discloses wherein the alert management system further responds to the request by supplying alert identifiers satisfying the request and whose description cannot be refined with respect to said request (Julisch: pages 464-465 and 467-468, section 7).

20. Regarding claim 5, Julisch as modified further discloses wherein the alert identifier is a pair consisting of an identifier of the intrusion detection sensor that produces the alert and an alert serial number assigned by said intrusion detection sensor (Julisch: pages 449 and 452).

21. Regarding claim 6, Julisch as modified further discloses wherein the content of each alert includes a text message supplied by a corresponding intrusion detection sensor (Julisch: pages 451-452).

22. Regarding claim 7, Julisch as modified further discloses wherein each valued attribute includes an attribute identifier and an attribute value (Julisch: pages 449 and 451-452).

23. Regarding claim 8, Julisch as modified further discloses wherein each attribute identifier is associated with one of the following attribute domains: attack domain, attacker identity domain, victim identity domain and attack date domain (Julisch: pages 449 and 451-452).

24. Regarding claim 9, Julisch as modified further discloses wherein the description of a given alert is completed by recovering recursively from generalization relationships of the taxonomic structures a set including more general valued attributes not already included in the description of another alert completed previously (Julisch: pages 449 and 456, last paragraph).

25. Regarding claim 10, Julisch as modified further discloses wherein the valued attributes in the taxonomic structure are organized in accordance with an acyclic directed graph (Julisch: pages 449 and 462).

26. Regarding claim 11, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

27. Regarding claim 12, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

28. Regarding claim 13, Julisch as modified further discloses Information security system comprising intrusion detection sensors and the alert management system according to claim 12 (Julisch: page 467-468).

Conclusion

29. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431